REMARKS

I. Rejection under 35 U.S.C. § 103

A. Claims 1-4, 6-9, and 11-19

Claims 1-4, 6-9, and 11-19 stand rejected under 35 U.S.C. § 102(b) as being anticipated by Barkan (European Patent Application No. EP 0738085) in view of Liao (US Patent No. 6263437). Applicants disagree.

Barkan discloses an "Apparatus for transferring the encryption key in a secure way, to facilitate establishing a secure communication link, comprises a key management device attaching to each user's encryption machine for the purpose of key distribution, and a secure encryption key distribution center. A key management device is attached to each user's encryption machine, containing a list of secure communication partners and their respective encryption keys. The encryption key and other parameters are transferred automatically to the encryption machine. The called machine receives the caller identification, and the encryption key and other parameters are transferred automatically. The device displays to each user the true, reliable identity of the other party. If the desired addressee data is not found in the local data list, the key management device connects a secure key distribution center. The communication with the key distribution center is protected by encryption using the public key method. The key distribution center creates, for each user, a "certificate" which includes the user public key, user identification and issue date, all encrypted with the center's private key. The certificate can be used to access a multitude of remote databases or other information services on an irregular basis, without the need to subscribe to all of them. It may be also used for secure payment over

insecure links using credit cards and/or for caller identification. The certificate method is used for flexible authorization schemes, to indicate changing time period of validity or authorizations/ permits."

Liao discloses "A crypto-ignition process is needed to establish an encrypted communication protocol between two devices connected by an insecure communication link. The present invention introduces a method of creating an identical secret key to two communicating parties is conducted between a thin device and a server computer over an insecure data network. The thin device generally has limited computing power and working memory and the server computer may communicate with a plurality of such thin devices. To ensure the security of the secret key on both sides and reduce traffic in the network, only a pair of public values is exchanged between the thin device and the server computer over the data network. Each side generates its own secret key from a self-generated private value along with the received counterpart's public value according to a commonly used key agreement protocol, such as the Diffie-Hellman key agreement protocol. To ensure that the generated secret keys are identical on both sides, a verification process is followed by exchanging a message encrypted by one of two generated secret keys. The secret keys are proved to be identical and secret when the encrypted message is successfully decrypted by the other secret key. To reduce network traffic, the verification process is piggybacked with a session request from the thin device to establish a secure and authentic communication session with the server computer. The present invention enables the automatic delivery of the secret keys, without requiring significant computing power and working memory, between each of the thin clients respectively with the server computer." (Liao, Abstract)

Applicants submit that Barkan and Liao fail to disclose "distributing the generated key to both telephony adapters", or "telephony adapters", as recited by Applicants' independent claims 1, 6, 11, and 15.

The present invention, in one embodiment, "provides a gateway controller that creates a media stream encryption key that is used to encrypt and decrypt messages between users. When a first user attempts to establish a secure channel with a second user, the gateway controller (source) associated with the first user, creates the media stream encryption key, sends the key inside a signaling message to the gateway controller (destination) that services the second user. The two gateway controllers then send the key to the two CTAs, that service the first and second user. This allows the two CTAs, and thus, the two users to quickly establish a secure communication channel in the IP telephony network." (See Applicants' Specification, page 2, lines 16-24)

(1) Barkan and Liao fail to teach, disclose, or suggest distributing the generated key to both telephony adapters, or the telephony adapters of the claims. (2) In addition, the combination of Barkan and Liao would not yield the present invention as claimed because the references are incompatible.

(1) *distributing the generated key to both telephony adapters*: The claims further call for the gateway controller to distribute the secret key to the both **telephony adapters**. The Office Action concedes that Barkan fails to teach the use of telephony adapters or that a key is distributed to telephony adapters. The Office Action then asserts that Liao reads on this limitation. However upon a search of the Liao reference, the Liao reference is completely devoid of the teaching, disclosure or suggestion of the use telephony adapters. However, the Office Action cites portions of Therefore, Barkan

clearly fails to teach what is recited in Applicants' claims. Namely, that the secret key is distributed from the gateway controller to both the first and second telephony adapters.

(2) *the references are incompatible and neither reference teaches generating a secret key at a gateway contoller*: Barkan describes a key distribution center which forwards the *public key* **from** the *addressee* **to** the *initiator*. (Barkan, col. 3, lines 17-25; col. 6, lines 35-40; col. 7, lines 45-50) Thus, in Barkan, the public key is forwarded to an initiator, but is distributed ***from***, instead of ***to***, the addressee. The Office Action asserts that Liao teaches generating a secret key at the first gateway controller, however, Liao actually teaches that "**each side generates its own secret key** from a self-generated private value along with the received counterpart's public value according to a commonly used key agreement protocol, such as the Diffie-Hellman key agreement protocol." As such, the references are incompatible because they teach different methods of key generation. In addition, both references still fail to teach what is recited by Applicant's claims since neither reference teaches generating a secret key at a gateway controller.

In view of the above arguments, Applicants submit that independent claims 1, 6, 11, and 15 are patentable over Barkan. Claims 2-4, 7-9, and 12-14, and 16-19 are patentable at least by virtue of depending from their respective base claim. Applicants respectfully request withdrawal of the rejection.

B. Claims 5 and 10

Claims 5 and 10 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Barkan and Liao in view of Ganesan (U.S. Patent No. 5,535,276, issued July 9, 1996) (Ganesan). Applicant respectfully disagrees.

As stated above in Section I. A., Barkan and Liao fails to disclose "generating a secret key at the gateway controller", "distributing the generated key to both telephony adapters", or "telephony adapters". In order to cure the Examiner's perceived deficiency of Barkan and Liao, Ganesan is cited.

Ganeson discloses a system and method for securing communications using split private key asymmetric cryptography. However, Ganeson, like Barkan and Liao, also fails to teach, disclose, or suggest "generating a secret key at the gateway controller", "distributing the generated key to both telephony adapters", or "telephony adapters", as recited in claims 1, 6, 11, and 15. As such, the combination of Barkan, Liao, and Ganeson fail to teach what is recited by Applicants' claims.

In view of the above arguments, Applicants submit that claims 5 and 10 are patentable over Barkan and Liao in view of Ganeson. Applicants respectfully request withdrawal of the rejection.

Conclusion

Having fully responded to the Office Action, the application is believed to be in condition for allowance. Should any issues arise that prevent allowance of the above application, the examiner is invited to contact the undersigned to resolve such issues.

To the extent an extension of time is needed for consideration of this response, Applicant hereby request such extension and, the Commissioner is hereby authorized to charge deposit account number 502117 for any fees associated therewith.

Date: July 23, 2007

Respectfully submitted,

By: /Thomas Bethea, Jr./
Thomas Bethea, Jr.
Reg. No.: 53,987

Motorola Connected Home Solutions
101 Tournament Drive
Horsham, PA 19044
(215) 323-1850